21224 cited PCT
2003321 cited EP

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 732 537**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **95 03859**

(51) Int Cl⁶ : H 04 N 7/16, 9/76, G 09 C 1/00

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 31.03.95.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 04.10.96 Bulletin 96/40.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *CANAL + SOCIETE ANONYME* — FR.

(72) **Inventeur(s)** : DUVERNE JACQUES.

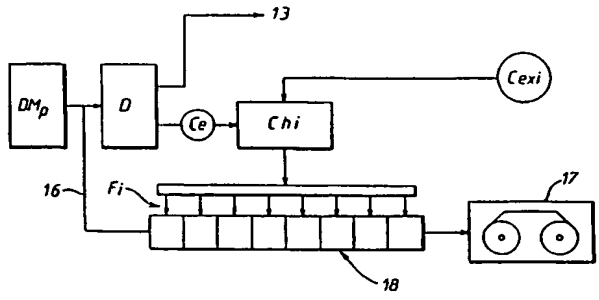
(73) **Titulaire(s)** :

(74) **Mandataire** : SABATIER.

(54) PROCEDE ET INSTALLATION D'ENREGISTREMENT D'INFORMATIONS NUMERIQUES CRYPTEES.

(57) Procédé d'enregistrement d'informations numériques cryptées, notamment des programmes de télévision, permettant de préserver les intérêts des ayants droit des oeuvres diffusées.

Selon l'invention, on enregistre dans un enregistreur (17) les informations numériques sous forme embrouillée après avoir remplacé la clé d'embrouillage des composantes d'exploitation desdites informations numériques par une clé d'embrouillage équivalente chiffrée par une clé d'exploitation interne (Cexi) spécifique à l'unité de décryptage associée à l'enregistreur, la substitution des clés pouvant se faire au moyen d'un registre à décalage (18).



FR 2 732 537 - A1

"Procédé et installation d'enregistrement d'informations numériques cryptées"

L'invention se rapporte à un procédé d'enregistrement d'informations numériques cryptées, notamment des programmes de télévision, diffusées sous forme cryptée depuis un centre d'émission jusqu'à des unités de décryptage où les informations numériques peuvent être décodées et restituées en clair, par exemple sur un écran de télévision.

L'invention concerne aussi une installation d'enregistrement d'informations numériques associant des moyens de décryptage à un enregistreur numérique.

On sait que l'enregistrement de programmes de télévision peut se faire pratiquement sans perte de qualité. Il en résulte une inquiétude légitime des ayants droit des oeuvres audiovisuelles susceptibles d'être diffusées sous forme numérique, par voie hertzienne ou par câble. En effet, une seule diffusion d'une oeuvre sur un tel réseau peut donner naissance à une activité de production de copies parfaitement reproductibles indéfiniment et sans dégradation, pour alimenter illégalement un marché d'enregistrements pirates. Jusqu'à présent, des solutions très imparfaites ont été mises en oeuvre. L'une d'elles consiste à caractériser chaque copie mise légalement en circulation par une "signature" qui permet de remonter jusqu'au fautif en cas de diffusion massive non autorisée. Cette pratique permet de réprimer

des agissements délictueux mais ne permet pas de prévenir le piratage commercial.

Par ailleurs, l'enregistrement de telles oeuvres en vue d'un usage privé, limité, selon l'expression consacrée, au "cercle familial", c'est-à-dire dépourvu de caractère commercial, est depuis longtemps toléré et doit pouvoir se poursuivre avec l'avènement de la télévision numérique.

L'invention permet, par le biais de la diffusion cryptée, de proposer un compromis équitable entre les intérêts légitimes des ayants droit des oeuvres diffusées et le respect de la liberté de copie à usage privé.

Plus précisément, l'invention concerne un procédé d'enregistrement d'informations numériques cryptées, par exemple des informations de télévision, diffusées sous forme cyptée depuis un centre d'émission comprenant des moyens de cryptage paramétrés par une clé d'embrouillage jusqu'à au moins une unité de décryptage comprenant des moyens de désembrouillage, lesdites informations numériques renfermant des composantes d'exploitation (ECM) définissant une clé d'embrouillage chiffrée par une clé d'exploitation, caractérisé en ce qu'il consiste à enregistrer lesdites informations numériques sous forme embrouillée après avoir remplacé la clé d'embrouillage chiffrée dans lesdites composantes d'exploitation par une clé d'embrouillage équivalente chiffrée par une clé d'exploitation interne, spécifique à ladite unité de décryptage.

Selon un mode d'exploitation préféré, le procédé consiste à déchiffrer la clé d'embrouillage valide à un

moment donné dans chaque composante d'exploitation, à la chiffrer à nouveau sous le paramétrage de ladite clé d'exploitation interne et à la réinsérer sous cette nouvelle forme chiffrée dans chaque composante d'exploitation à la place de ladite clé d'embrouillage valide.

L'invention concerne également une installation d'enregistrement d'informations numériques cryptées, par exemple des programmes de télévision, diffusées sous forme cryptée depuis un centre d'émission comprenant des moyens de cryptage paramétrés par une clé d'embrouillage, du type comprenant un enregistreur numérique relié à une unité de décryptage comportant des moyens de débrouillage, lesdites informations numériques renfermant des composantes d'exploitation (ECM) définissant une clé d'embrouillage chiffrée par une clé d'exploitation, caractérisée en ce que l'entrée d'enregistrement dudit enregistreur numérique est connectée à une ligne de transmission desdites informations numériques embrouillées via des moyens de substitution aptes à remplacer ladite clé d'embrouillage d'une composante d'exploitation par une clé d'embrouillage équivalente paramétrée par une clé d'exploitation interne, spécifique à ladite unité de décryptage.

L'invention sera mieux comprise et d'autres avantages de celle-ci apparaîtront plus clairement à la lumière de la description qui va suivre d'un exemple de réalisation possible conforme à son principe, donnée uniquement à titre d'exemple, et faite en référence aux dessins annexés dans

lesquels:

- la figure 1 est un schéma-bloc de principe illustrant un système de diffusion d'informations numériques cryptées avec une unité de décryptage susceptible de recevoir, décoder et exploiter ces informations;

- la figure 2 illustre la nature des informations numériques transmises; et

- la figure 3 illustre, sous forme de schéma-bloc, les moyens spécifiques à l'invention, qui complètent chaque unité de décryptage pour permettre l'enregistrement conforme au principe de l'invention.

Un système de transmission cryptée d'informations numériques, en particulier de programmes de télévision à images numérisées est illustré. Il comprend une unité de cryptage 11 associée à un centre d'émission et une unité de décryptage 12 confiée à un abonné et constituant un décodeur; cette unité de décryptage est reliée à un récepteur 13 de visualisation, typiquement un récepteur de télévision, après conversion numérique-analogique. Chaque abonné possède donc une telle unité de décryptage 12. Un réseau de communication 15 est établi entre l'unité de cryptage 11 et l'unité de décryptage ou décodeur 12. Il s'agit par exemple d'un système de transmission par faisceau Hertzien, éventuellement relayé par satellite, ou d'un réseau câblé de distribution de programmes.

Les informations numériques N représentatives d'un programme sont constituées, comme le montre la figure 2,

d'une succession de messages transmis séquentiellement et comportant chacun une composante V représentative de l'image, une composante S représentative du son, éventuellement une composante T renfermant des informations de télétexte. La diffusion est dite "à accès contrôlé" lorsqu'au moins une composante V, S ou T (généralement les trois) est embrouillée à l'émission. Des composantes d'exploitation appelés ci-après "composantes ECM", (de l'anglais "Entitlement Control Message") complètent les composantes identifiées ci-dessus pour former, chaque fois, un message précité. Il est à noter que, très généralement, le réseau de communication 15 transmet simultanément une pluralité de programmes, cryptés ou non. Les messages d'informations représentatifs de ces programmes sont multiplexés à l'émission par un multiplexeur Mp et chaque décodeur comporte un démultiplexeur d'entrée DMp chargé de restituer les informations (selon la configuration de la figure 2) correspondant au programme choisi par l'abonné. Le multiplexeur Mp reçoit donc, entre autres, les informations délivrées par un embrouilleur E de l'unité de cryptage 11. Cet embrouilleur reçoit sur une entrée e les informations numériques N et les soumet à un algorithme mettant en oeuvre un paramètre dit "clé d'embrouillage" Ce.

Cette clé d'embrouillage est délivrée à l'embrouilleur et sous forme chiffrée par un chiffreur Ch_1 est adressée à l'unité de décryptage 12, via le réseau de communication 15 pour piloter un déchiffreur Dch_1 apte à restituer la clé Ce qui est appliquée en tant que paramètre à un

désembrouilleur D de l'unité de décryptage 12. Ce désembrouilleur, en présence de la même clé Ce, qui est validée à l'émission, est capable de soumettre les données numériques reçues du démultiplexeur DMp à un algorithme inverse de celui de l'embrouilleur pour restituer les informations numériques en clair. Celles-ci sont appliquées à une entrée du récepteur 13, (via des moyens de conversion numérique/analogique, non représentés) pour être reproduites, ici en tant que programme de télévision.

Le cryptogramme de la clé d'embrouillage Ce entre dans la constitution (avec les critères d'accès à la ou les composantes embrouillées) des composantes ECM indiqués ci-dessus. Par sécurité, la clé d'embrouillage est modifiée périodiquement (par exemple toutes les 10 secondes), par le chiffreur Ch_1 sous la commande d'une clé d'exploitation Cex. Celle-ci est aussi chiffrée par un chiffreur Ch_2 de façon à être transmise, par exemple par téléchargement, à l'unité de décryptage 12, jusqu'à un déchiffreur Dch_2 capable de restituer la clé d'exploitation Cex applicable au déchiffreur Dch_1.

Comme mentionné précédemment, la clé d'embrouillage Ce change assez fréquemment (10 secondes) pour lutter efficacement contre le piratage; elle est répétée plusieurs fois par seconde dans les ECM pour permettre un décodage immédiat dès que l'abonné sélectionne le programme correspondant. En revanche, la clé d'exploitation Cex n'est modifiée qu'au bout d'une période de temps plus longue, par exemple de l'ordre d'un mois. Cette opération se fait sous

le contrôle d'une clé de gestion Cg personnalisée pour chaque abonné.

Les différentes clés Ce, Cex et déchiffreurs Dch_1, Dch_2 associés sont intégrés dans un module de sécurité de l'unité de décryptage 12, et sont donc inaccessibles au détenteur du décodeur.

L'invention s'inscrit dans le cadre de l'exploitation d'un système de ce genre et vise à permettre la copie d'un programme sous forme numérisée en vue d'un usage exclusivement à titre privé. En effet, on sait que l'enregistrement vidéo d'un programme numérisé peut être fait pratiquement sans dégradation de qualité et qu'un diffuseur de tels programmes numérisés pourrait devenir une source de duplication, portant préjudice aux ayants droit des oeuvres audiovisuelles diffusées.

Dans un tel système, on n'a jusqu'à présent jamais envisagé d'enregistrer le programme sous sa forme embrouillée. En effet, un tel programme ne serait plus lisible après le premier changement de la clé d'exploitation intervenant après son enregistrement.

L'idée de base de l'invention consiste au contraire à tirer parti d'un enregistrement numérique d'un programme sous forme embrouillée en utilisant cet embrouillage pour réserver la relecture à l'usage exclusif de l'abonné qui a réalisé ledit enregistrement. Pour ce faire, l'unité de décryptage 12 comporte une dérivation 16 de signal numérique embrouillé, en amont du désembrouilleur D, reliée à la ligne d'enregistrement d'un enregistreur numérique 17

tel qu'un magnétoscope et dans laquelle sont intercalés des moyens de substitution des composantes ECM, aptes à remplacer les ECM qui sont transmis, par de nouveaux ECM contenant une clé d'embrouillage équivalente chiffrée par une clé d'exploitation dite "interne" Cexi, propre à l'abonné. Cette clé Cexi, spécifique, est différente pour chacun des usagers, c'est-à-dire intégrée au module de sécurité du décodeur. Dans la pratique, ces moyens seront par exemple constitués par un simple registre à décalage 18 (figure 3) dans lequel défilent les messages issus de la sortie du multiplexeur DMp. Lorsque la composante ECM d'un message traverse ce registre à décalage, les entrées de forçage Fi sont commandées pour placer tous les étages concernés du registre dans des états représentant une clé d'embrouillage chiffrée par ladite clé d'exploitation interne.

Plus précisément, le désembrouilleur D comporte une sortie où la clé d'embrouillage Ce, valide à un moment donné de l'enregistrement, est disponible. Cette clé d'embrouillage pilote un chiffreur interne Chi paramétré par la clé d'exploitation interne Cexi. La sortie du chiffreur interne pilote les entrées de forçage du registre à décalage pour inscrire le cryptogramme de la nouvelle clé d'embrouillage chiffrée par la clé d'exploitation interne Cexi. Les autres composantes embrouillées V, S et T ne sont pas modifiées et la succession des messages représentatifs d'un programme est enregistrée sous cette forme, c'est-à-dire avec des composantes ECM modifiées comme indiqué.

A la reproduction, il suffit de brancher la sortie numérique de l'enregistreur à l'entrée du désembrouilleur D et de paramétrer le déchiffreur Dch_1 par la clé d'exploitation interne Cexi, se substituant à la clé Cex.

REVENDICATIONS

1- Procédé d'enregistrement d'informations numériques cryptées, par exemple des informations de télévision diffusées sous forme cyptée depuis un centre d'émission (11) comprenant des moyens de cryptage paramétrés par une clé d'embrouillage jusqu'à au moins une unité de décryptage (12) comprenant des moyens de désembrouillage, lesdites informations numériques renfermant des composantes d'exploitation (ECM) définissant une clé d'embrouillage (Ce) chiffrée par une clé d'exploitation, caractérisé en ce qu'il consiste à enregistrer (17) lesdites informations numériques sous forme embrouillée après avoir remplacé la clé d'embrouillage chiffrée dans lesdites composantes d'exploitation par une clé d'embrouillage équivalente chiffrée par une clé d'exploitation interne (Cexi), spécifique à ladite unité de décryptage.

2- Procédé selon la revendication 1, caractérisé en ce qu'il consiste à déchiffrer ladite clé d'embrouillage (Ce) valide dans chaque composante d'exploitation, à la chiffrer (Chi) à nouveau sous le paramétrage de ladite clé d'exploitation interne et à la réinsérer (18) sous cette nouvelle forme chiffrée dans chaque composante d'exploitation à la place de ladite clé d'embrouillage valide.

3- Procédé selon la revendication 2, caractérisé en ce qu'il consiste à faire circuler lesdites informations numériques embrouillées dans un registre à décalage (18),

avant de les enregistrer et à piloter des entrées de forçage (Fi) dudit registre à décalage pour y inscrire ladite clé d'embrouillage équivalente lorsque ledit registre renferme ladite clé d'embrouillage valide.

4- Installation d'enregistrement d'informations numériques cryptées, par exemple des programmes de télévision, diffusées sous forme cryptée depuis un centre d'émission (11) comprenant des moyens de cryptage paramétrés par une clé d'embrouillage, du type comprenant un enregistreur numérique (17) relié à une unité de décryptage comportant des moyens de débrouillage (D), lesdites informations numériques renfermant des composantes d'exploitation (ECM) définissant une clé d'embrouillage chiffrée par une clé d'exploitation, caractérisée en ce que l'entrée d'enregistrement dudit enregistreur numérique (17) est connectée à une ligne de transmission desdites informations numériques embrouillées via des moyens de substitution (18) aptes à remplacer ladite clé d'embrouillage d'une composante d'exploitation par une clé d'embrouillage équivalente paramétrée par une clé d'exploitation interne (Cexi), spécifique à ladite unité de décryptage (12).

5- Installation selon la revendication 4, caractérisée en ce que ladite ligne de transmission (16) desdites informations numériques embrouillées est connectée en amont desdits moyens de débrouillage et comporte un registre à décalage (18) dans lequel transitent lesdites informations numériques embrouillées, en ce que lesdits moyens de

débrouillage comportent une sortie où est délivrée ladite clé d'embrouillage (Ce) déchiffrée et en ce qu'un chiffreur interne (Chi) pilote des moyens de forçage dudit registre à décalage, ledit chiffreur interne étant relié à ladite sortie délivrant ladite clé d'embrouillage déchiffrée.

6- Installation selon la revendication 5, caractérisée en ce que le chiffreur interne (Chi) est paramétré par ladite clé d'exploitation interne (Cexi) et délivre des informations de forçage au registre à décalage, représentatif de ladite clé d'embrouillage chiffrée par ladite clé d'exploitation interne, lorsque ledit registre contient des informations de clé d'embrouillage d'une composante d'exploitation (ECM).

FIG.1

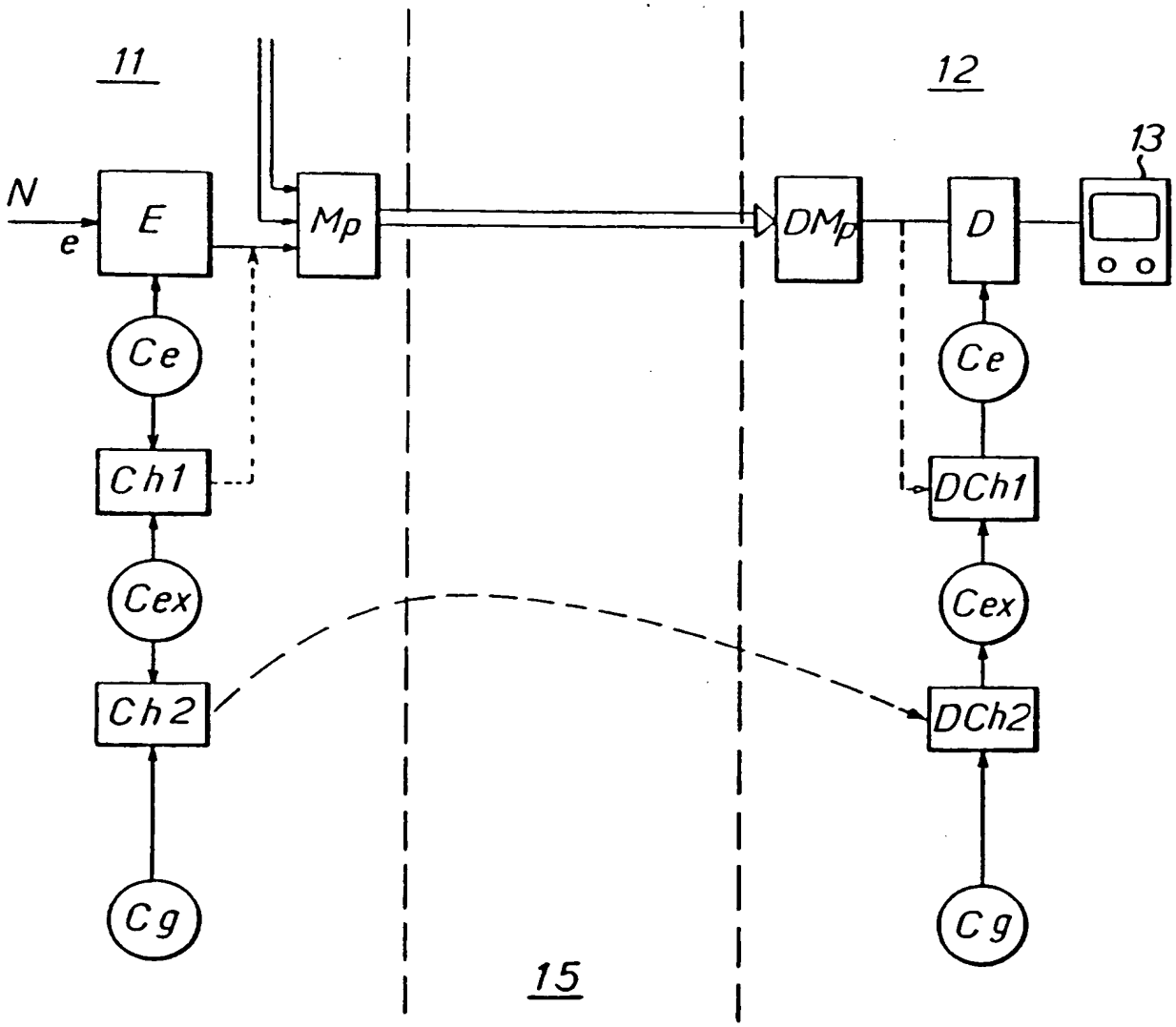


FIG. 2

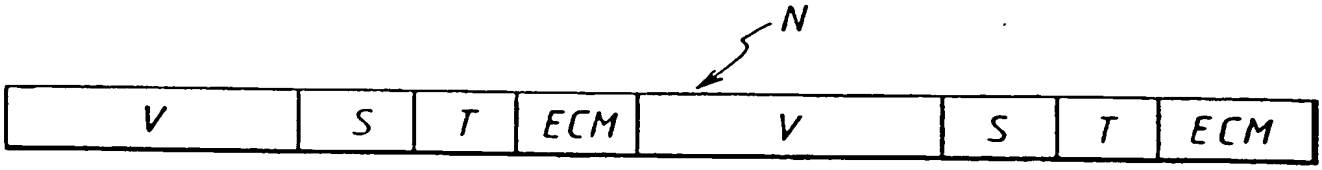
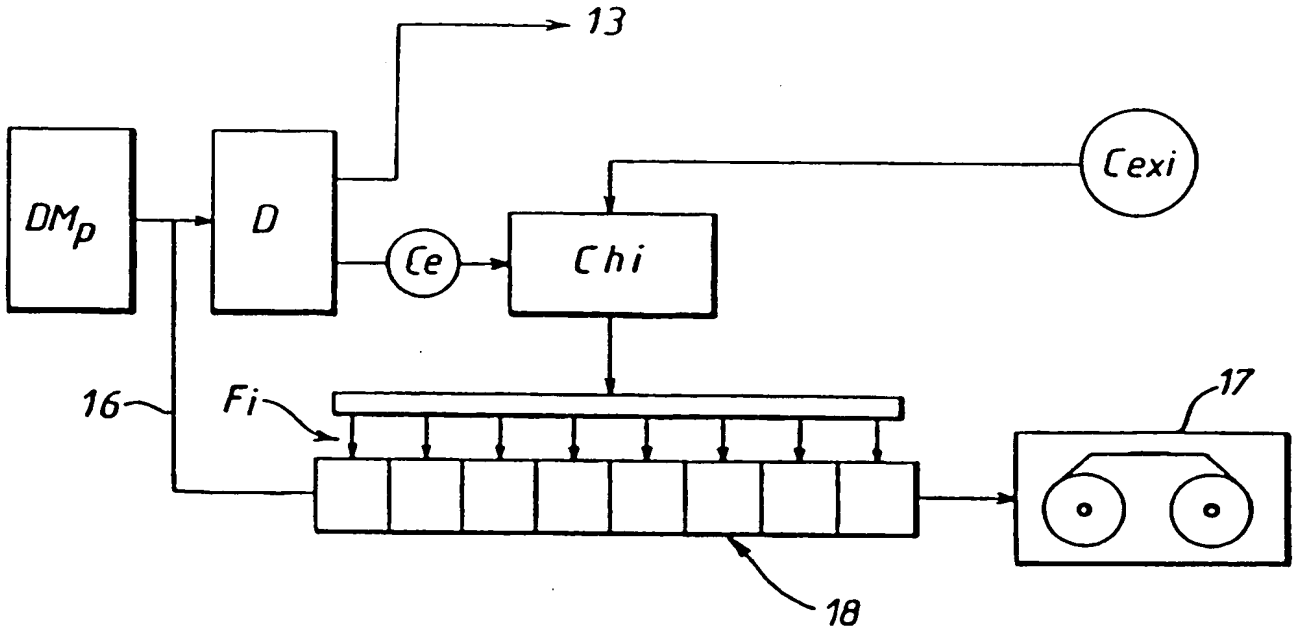


FIG. 3



REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2732537
N° d'enregistrement national

FA 516352
FR 9503859

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	CABLE TV SESSIONS, MONTREUX, JUNE 10 - 15, 1993, no. SYMP. 18, 11 Juin 1993 POSTES;TELEPHONES ET TELEGRAPHES SUISSES, pages 761-769, XP 000379391 VIGARIE J P 'A DEVICE FOR REAL-TIME MODIFICATION OF ACCESS CONDITIONS IN A D2-MAC/PACKET EUROCRYPT SIGNAL: THE TRANSCONTROLLER' * le document en entier * ---	1-6
A	PATENT ABSTRACTS OF JAPAN vol. 014 no. 200 (E-0920) ,24 Avril 1990 & JP-A-02 041051 (MATSUSHITA ELECTRIC IND CO LTD;OTHERS: 01) 9 Février 1990, * abrégé * ---	1-6
A	US-A-5 230 019 (YANAGIMICHI TOYOKAZU ET AL) 20 Juillet 1993 * abrégé * ---	1-6
A	EP-A-0 461 029 (MATRA COMMUNICATION ;FRANCE TELECOM (FR); TELEDIFFUSION FSE (FR)) 11 Décembre 1991 * le document en entier * -----	1-6

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

H04N

Date d'achèvement de la recherche	Examinateur
9 Octobre 1995	Greve, M

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)